Technical Cybersecurity

Credential Stealing

Remote Exploitation is Cool

Credential theft is much easier

- Credentials are available on the black market
- They’re saved on systems
- They are recognizable, relatively short words

How to Acquire

GET THEM FROM THE FILESYSTEM

- Linux system? /etc/password or /etc/shadow
- Windows? LANMAN, NT, wire protocols
- Others? Kerberos, Databases, etc.

JOHN THE RIPPER, HASHCAT, CAIN

- Tools to decrypt passwords

John the Ripper

LINUX OR WINDOWS

- John is multi-platform and has same options on all

DISPLAYED AND STORED

- Cracked passwords will be displayed on the screen and cached in the john.pot file

MONITOR STATUS

- Press any key, get run status
- Number of guesses, time to run, percentage finished, combinations tested per second, current range of passwords being tried

Hashcat

ANOTHER PASSWORD CRACKER

- Faster, more powerful, harder to use
- Implements over 200 password algorithms
- Can use GPUs
- Multiplatform

REQUIRES YOU TO SPECIFY ALGORITHM TO CRACK

- **$ hashcat64 —help** will show you a list of them

OTHER OPTIONS

- hashcat.potfile (cracked passwords)
- Multiple dictionary files
- Word mangling rules

Case: BlackEnergy3

ADVANCED PERSISTENT THREAT

- Targeted Ukranian energy facilities
- Initially gained entry via trojan distributed in a word document
- Installed network scanners, keyboard loggers, password stealer, recon tools
- Used cracked and stolen passwords that users had reused across multiple systems (a very common problem!)

Next up, Cain.